

# Dial One for Scam: A Large-Scale Analysis of **Technical Support Scams**



Najmeh Miramirkhani

Oleksii Starov

Nick Nikiforakis

# What are Tech Support Scams?

# Tech Support Scam Evolution

3

2008

Fake support cold calls

2013

A Twist: Scammers started to use malvertising

2014

IC3 issued a public service announcement

2014

Microsoft sued several campaigns

2015

FTC took down several big campaigns

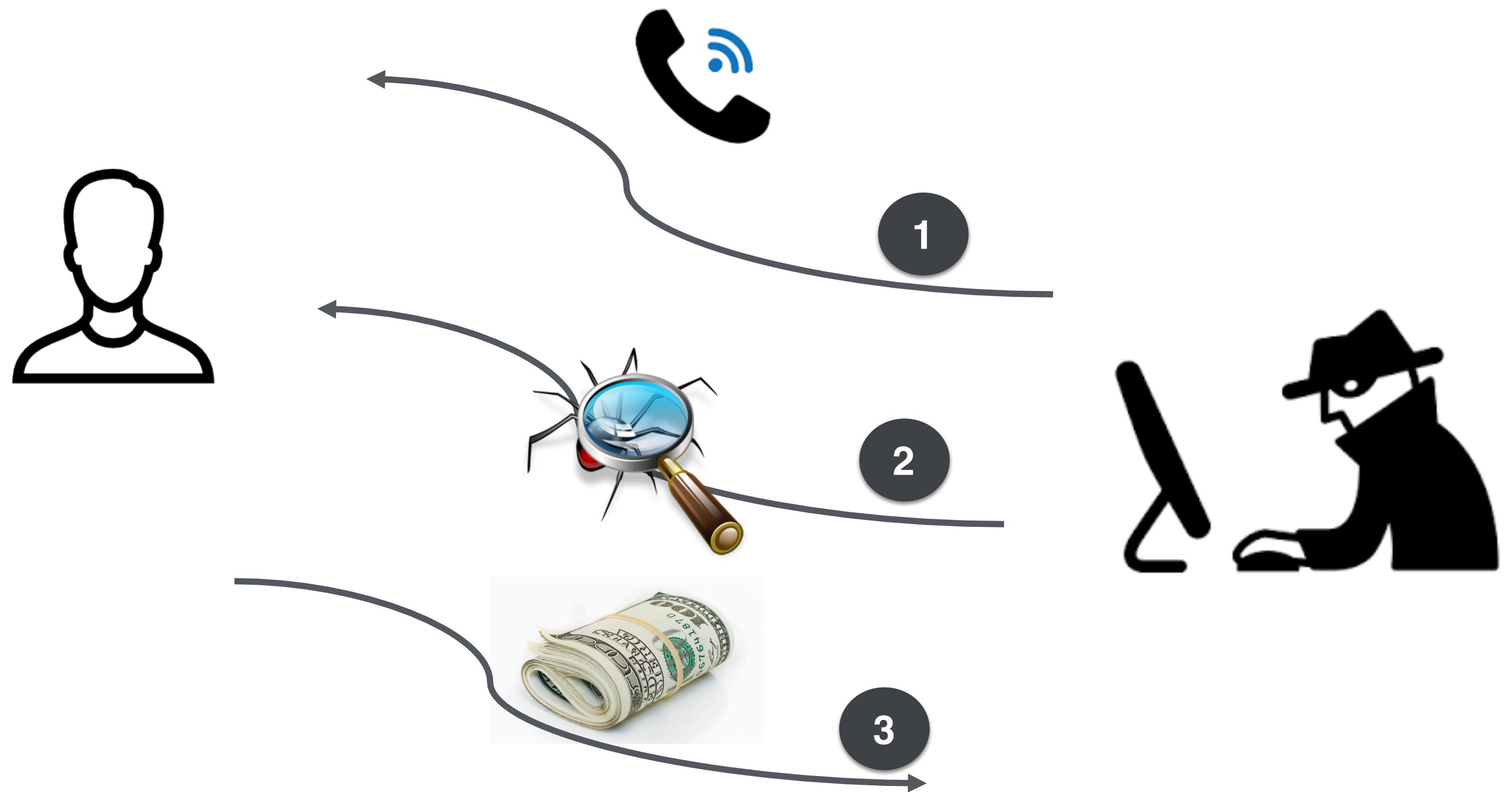
2016

IC3 issued a public service announcement

2017

Got more aggressive and still an increasing threat

# Tech Support Scam (Cold Calls)



# Tech Support Scam Evolution

5

2008

Fake support cold calls

2013

A Twist: Scammers started to use malvertising

2014

IC3 issued a public service announcement

2014

Microsoft sued several campaigns

2015

FTC took down several big campaigns

2016

IC3 issued a public service announcement

2017

Got more aggressive and still an increasing threat

# Tech Support Scam (malvertising)



locked concealed significant page password response continue com trick cause identity copyright major

engineering technical technicians visit

warning situation services connection fix

blocked classified reserved connection fix

shut contacting tracking logs live apply based deleted

stalkers unknown attention breach carry

frame location unknown address hacked www port

virus worms using email desk duped run

financial financial exposed wrong

malware social software

removed installed registry frame virus access restart

tcplocation worms viruses harmful info rightsharmful crash computing often

actions acts suspended prevent inject

calling dear pop communications webcam

current current administrator adware

acts acts suspended prevent inject

viruses viruses harmful info rightsharmful crash computing often

rightsharmful crash computing often

browsing restart program warriors

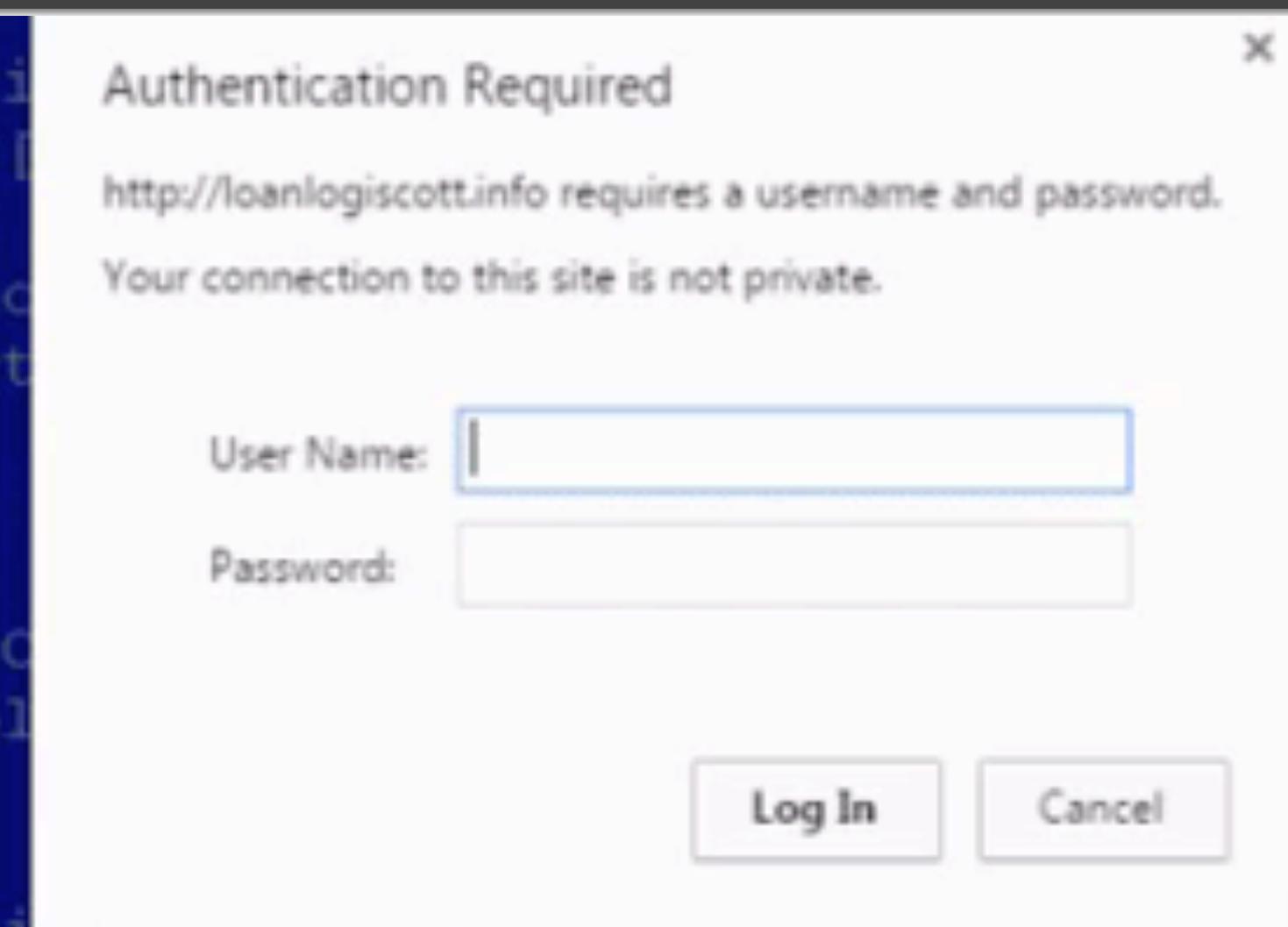
passwords especially causing something containing

details type logins useful reason anonymous hard



# Tech Support Scam Page(I)

```
* Starting System V initialisation compatibility[ OK ]
* Stopping flush early job output to logs[ OK ]
* Starting D-Bus system message bus[ OK ]
* Starting SystemD login management service[ OK ]
* Starting Bridge file events into upstart[ OK ]
* Starting system logging daemon[ OK ]
* Starting early crypto disks...
[ OK ]
* Starting Handle applying cloud-config[ OK ]
Skipping profile in /etc/apparmor.d/disable/
* Starting AppArmor profiles
[ OK ]
* Stopping System V initialisation compatibility[ OK ]
* Starting System V runlevel compatibility[ OK ]
* Starting save kernel messages[ OK ]
* Starting configure network device security[ OK ]
* Starting OpenSSH server[ OK ]
* Starting ACPI daemon[ OK ]
* Starting regular background program processing daemon[ OK ]
* Starting deferred execution scheduler[ OK ]
* Stopping save kernel messages[ OK ]
* Starting CPU interrupts balancing daemon[ OK ]
* Starting configure virtual network devices[ OK ]
* Starting automatic crash reporting application[ OK ]
Cloud-init v. 0.7.5 running '
```



Potential breaking attempt!

please call:

+1-866-793-2591



# Tech Support Scam Evolution

8

2008	Fake support cold calls
2013	A Twist: Scammers started to use malvertising
2014	IC3 issued a public service announcement
2014	Microsoft sued several campaigns
2015	FTC took down several big campaigns
2016	IC3 issued a public service announcement
2017	Got more aggressive and still an increasing threat

# Tech Support Scam Evolution

,

2008	Fake support cold calls
2013	A Twist: Scammers started to use malvertising
2014	IC3 issued a public service announcement
2014	Microsoft sued several campaigns
2015	FTC took down several big campaigns
2016	IC3 issued a public service announcement
2017	Got more aggressive and still an increasing threat

# Growth of 200%

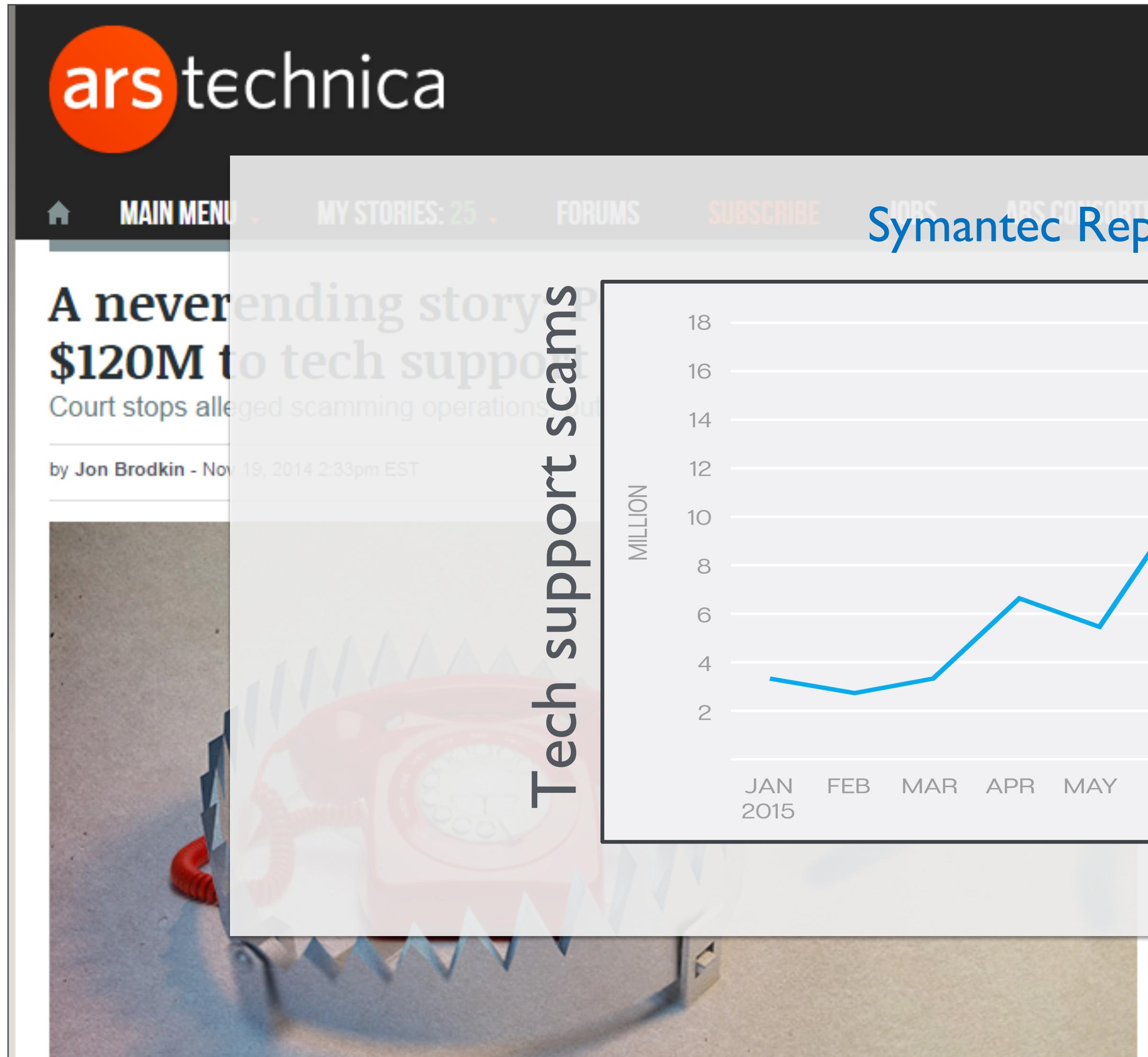
10

The screenshot shows the Ars Technica homepage with a dark header featuring the site's logo. Below the header is a navigation bar with links for 'MAIN MENU', 'MY STORIES: 25', 'FORUMS', 'SUBSCRIBE', 'JOBS', and 'ARS CONSORTIUM'. The main article title is 'A neverending story: PC users lose another \$120M to tech support scams'. A subtext below the title reads 'Court stops alleged scamming operations, but an end to the problem is elusive.' The author is Jon Brodkin, and the date is Nov 19, 2014, 2:33pm EST. Social sharing buttons for Facebook and Twitter are present, along with a comment count of 70. The featured image is a red rotary phone caught in a bear trap.

The screenshot shows a TechCrunch news article titled 'Microsoft takes on tech support scammers'. The article is dated December 19, 2014, and is categorized under 'Technology'. The main headline is 'Microsoft takes on tech support scammers'. The author is Jon Brodkin, and the date is Nov 19, 2014, 2:33pm EST. The image is a red rotary phone caught in a bear trap.

The screenshot shows a Network World news article titled 'FTC takes out “tech support” scammers; \$5.1 million in fines, retribution'. The author is Michael Cooney, and the date is Nov 19, 2014, 2:33pm EST. The main headline is 'FTC takes out “tech support” scammers; \$5.1 million in fines, retribution'. The author's profile picture is shown, and there is a link to 'About' the author.

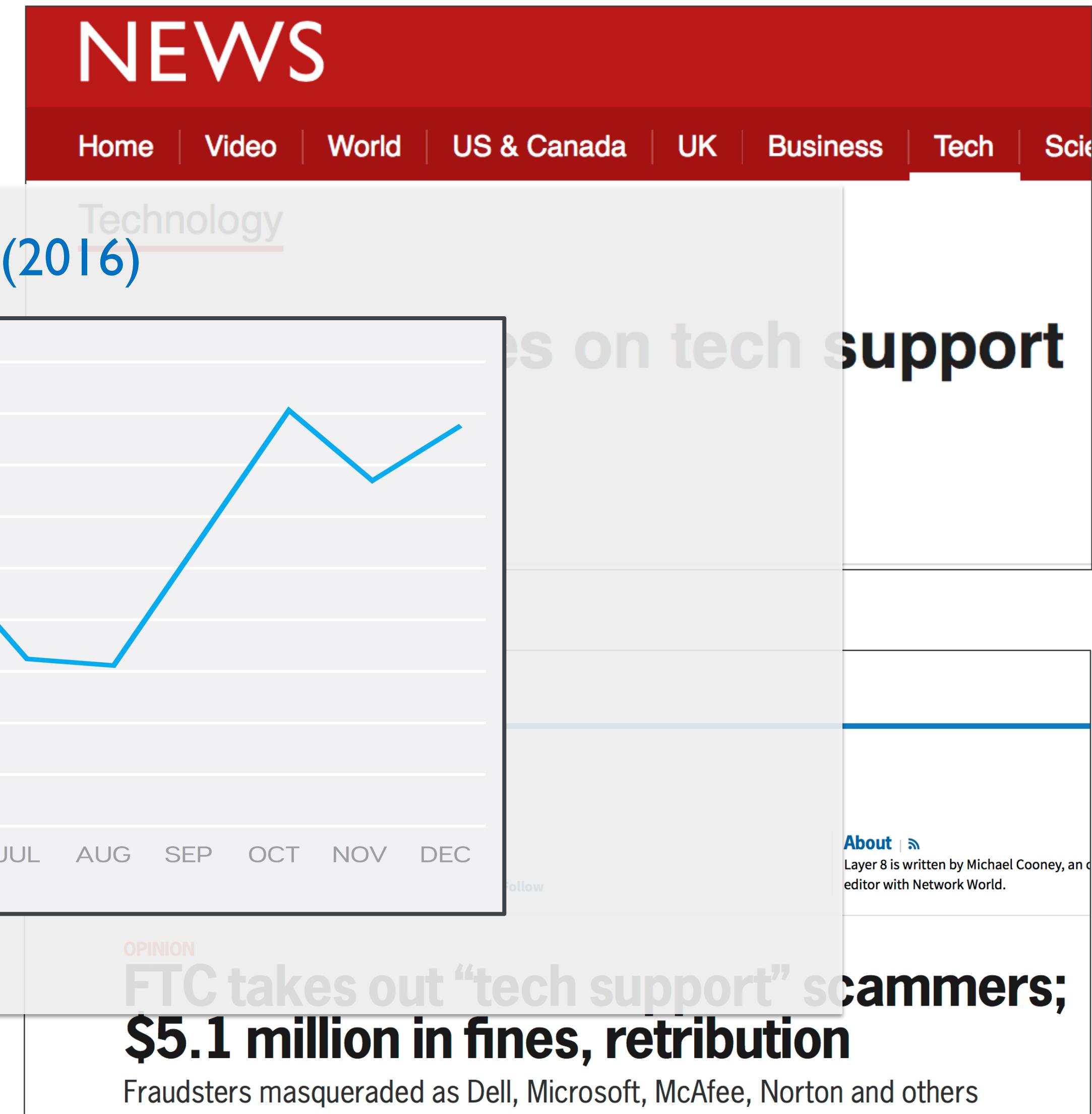
# Growth of 200%



A screenshot of an Ars Technica news article. The title is "A never-ending story: \$120M to tech support scams". The subtitle reads "Court stops alleged scamming operation". The author is Jon Brodkin, published on Nov 19, 2014 at 2:33pm EST. The main image shows a close-up of a computer keyboard with a red and blue gear graphic overlaid.

**Tech support scams**

Month	Value (Millions)
JAN 2015	3.5
FEB	2.8
MAR	3.5
APR	6.8
MAY	5.5
JUN	10.5
JUL	6.5
AUG	6.2
SEP	11.5
OCT	16.0
NOV	13.5
DEC	15.5



The top navigation bar includes links for Home, Video, World, US & Canada, UK, Business, Tech, and Science. The main headline is "Symantec Report (2016)". Below it is a chart titled "Tech support scams" showing monthly values from January 2015 to December. A sidebar on the right contains a link to "About" and a quote from Michael Cooney.

**Technology**

**Symantec Report (2016)**

**Tech support scams**

Month	Value (Millions)
JAN 2015	3.5
FEB	2.8
MAR	3.5
APR	6.8
MAY	5.5
JUN	10.5
JUL	6.5
AUG	6.2
SEP	11.5
OCT	16.0
NOV	13.5
DEC	15.5

**OPINION**

**FTC takes out “tech support” scammers; \$5.1 million in fines, retribution**

Fraudsters masqueraded as Dell, Microsoft, McAfee, Norton and others

# Research Goals

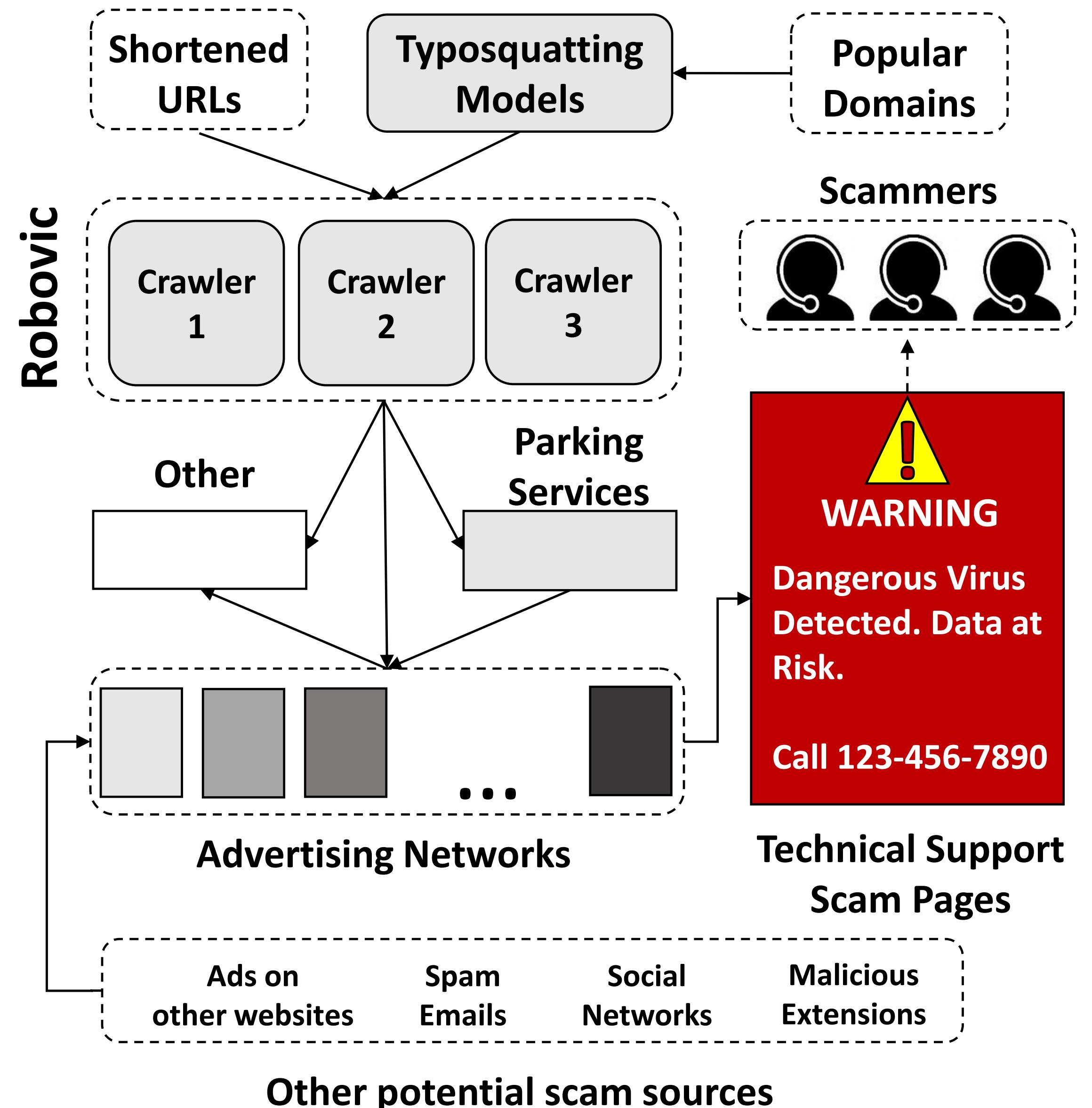
12

- Systematic study of Tech Support Scam ecosystem
- To investigate the:
  - Prevalence
    - # Domains, # Phone Numbers, and #Scam Campaigns
  - Details about the underlying infrastructure
    - Hosting providers, ASes, and Telecommunication companies
  - Evasion and social engineering techniques
    - Tools used, call-center infrastructures, and prices

# Tool Design (Robovic)

# Data Collection Methodology

14



# Collected Scam Domains

15

- Over 8 months

- Crawled 8 Million domains
- Resolved 5 Million domains
- Detected 22,000 scam URLs
- Extracted 8,600 unique scam domains
- 1500 phone numbers

## Short and readable domains

- computer-warning-message[.]com
- donotclose[.]website
- input-error[.]net

## Long with readable parts

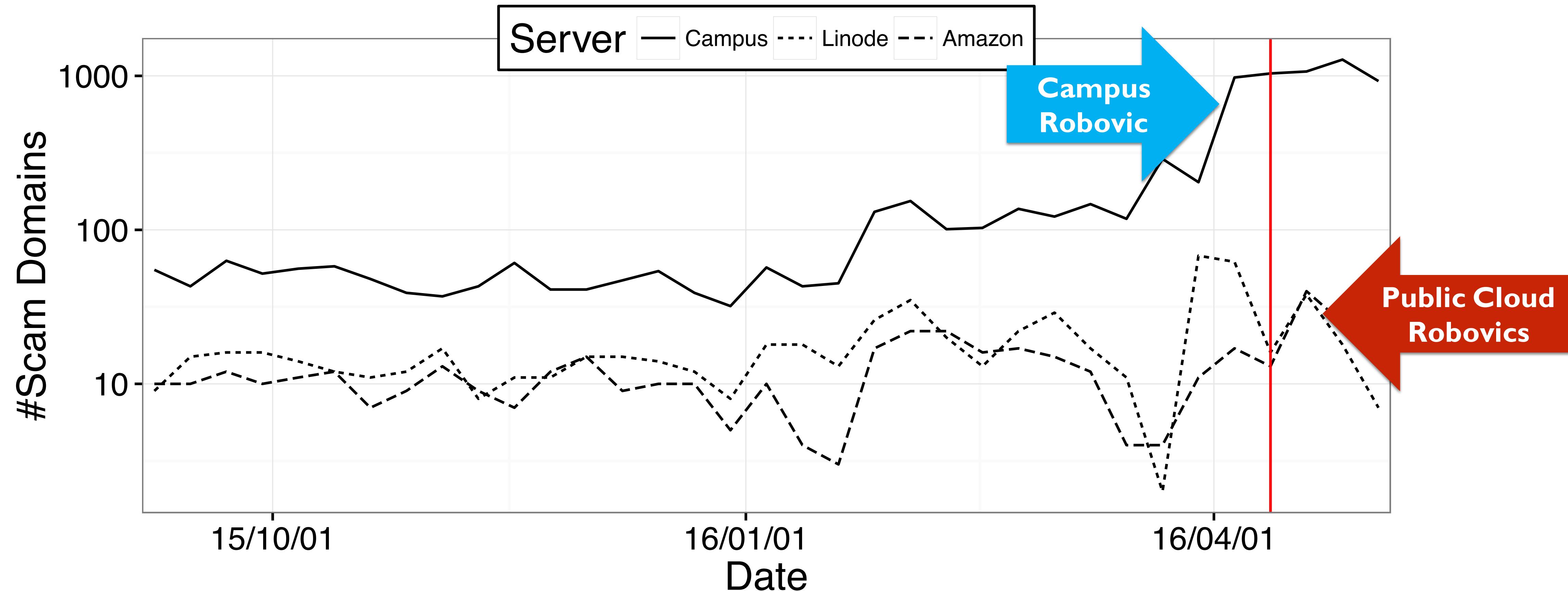
- 10.computerhaveaseriousproblempleasecallon18776431254t  
ollfree.yourcomputerhaveaseriousproblempleasecallon187764  
31254tollfree.yourcomputerhaveaseriousproblempleasecallon  
18776431254tollfree.browsersecurity16[.]club

## URLs from CDNs

- 1073964613.rsc.cdn77[.]org
- 924983738.r.cdnsun[.]net

# Weekly Scam Domains

16



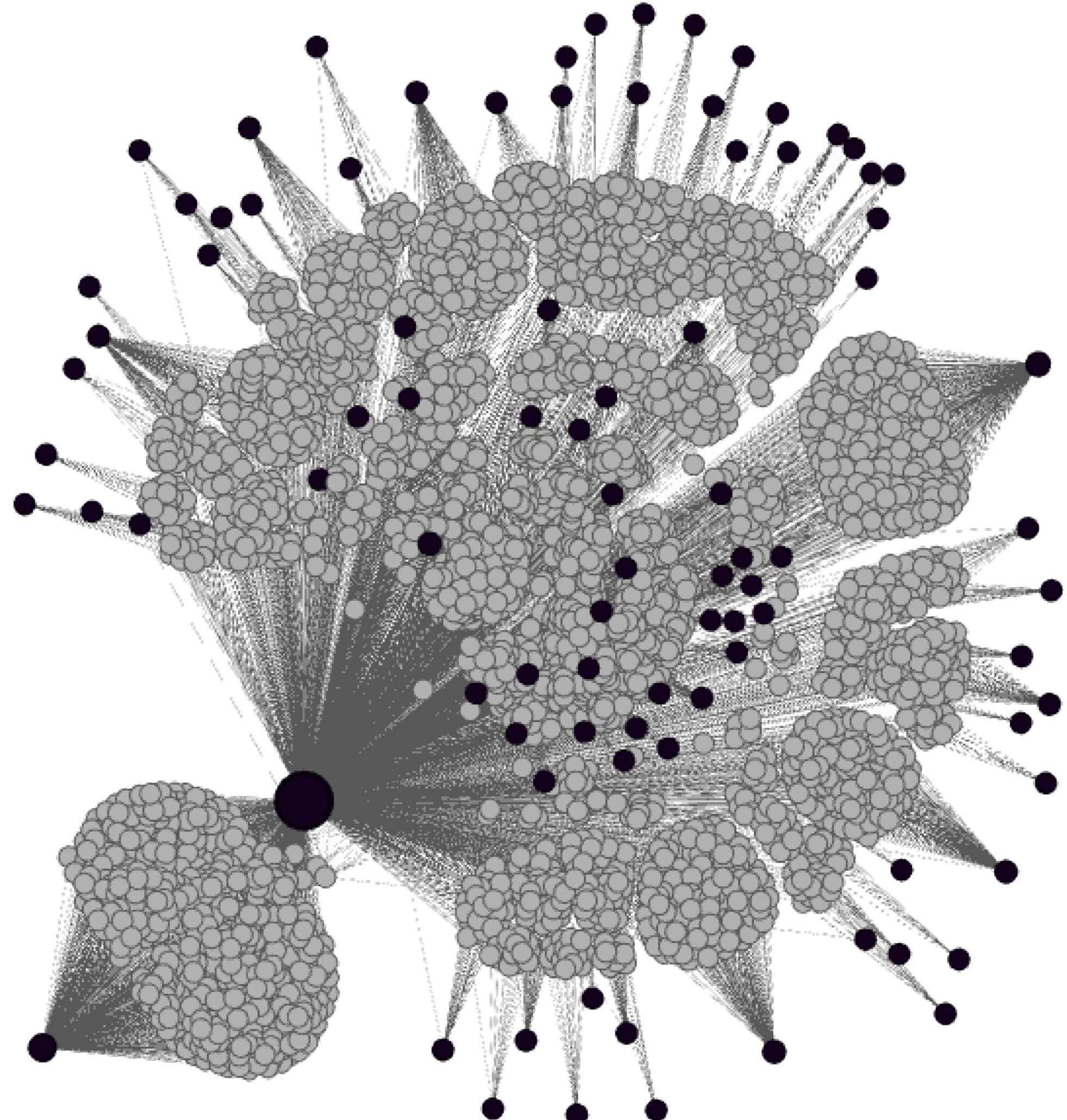
# Scam Domains & phone Numbers

17

- Hiding backend servers (16% used Cloudflare)
- Anonymized registration information (55%)
- Abuse a small number of Telco companies
  - 80% of numbers belong to Twilio, RingRevenue (Invoca), WilTel
  - Prefer those that provide APIs
    - Scalable solution for the scammers' business
- Number of phone numbers is much less than the number of domains
  - Phone numbers can link together domains of the same campaign

# Scam Campaigns

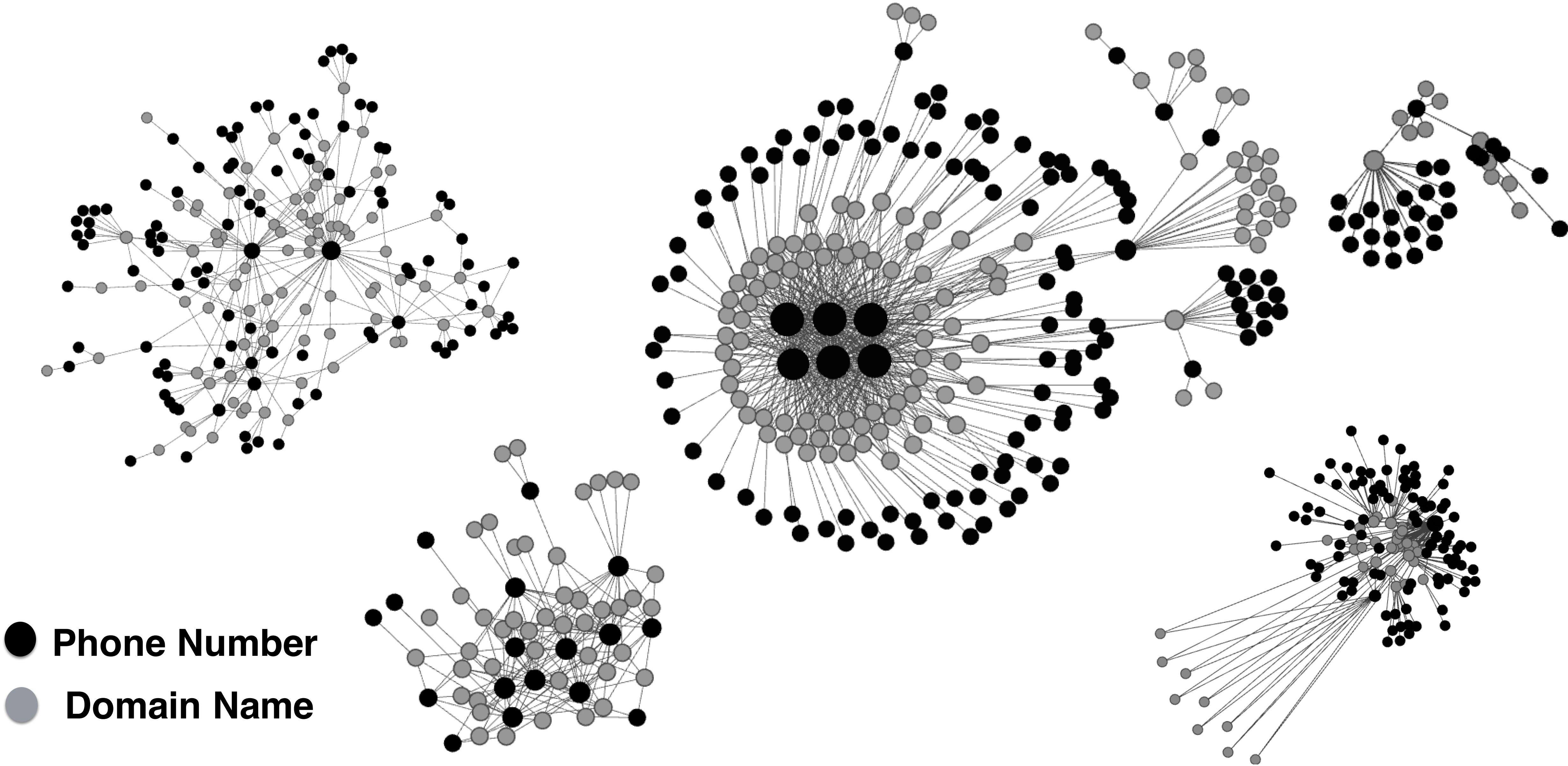
18



- Phone Number
- Domain Name

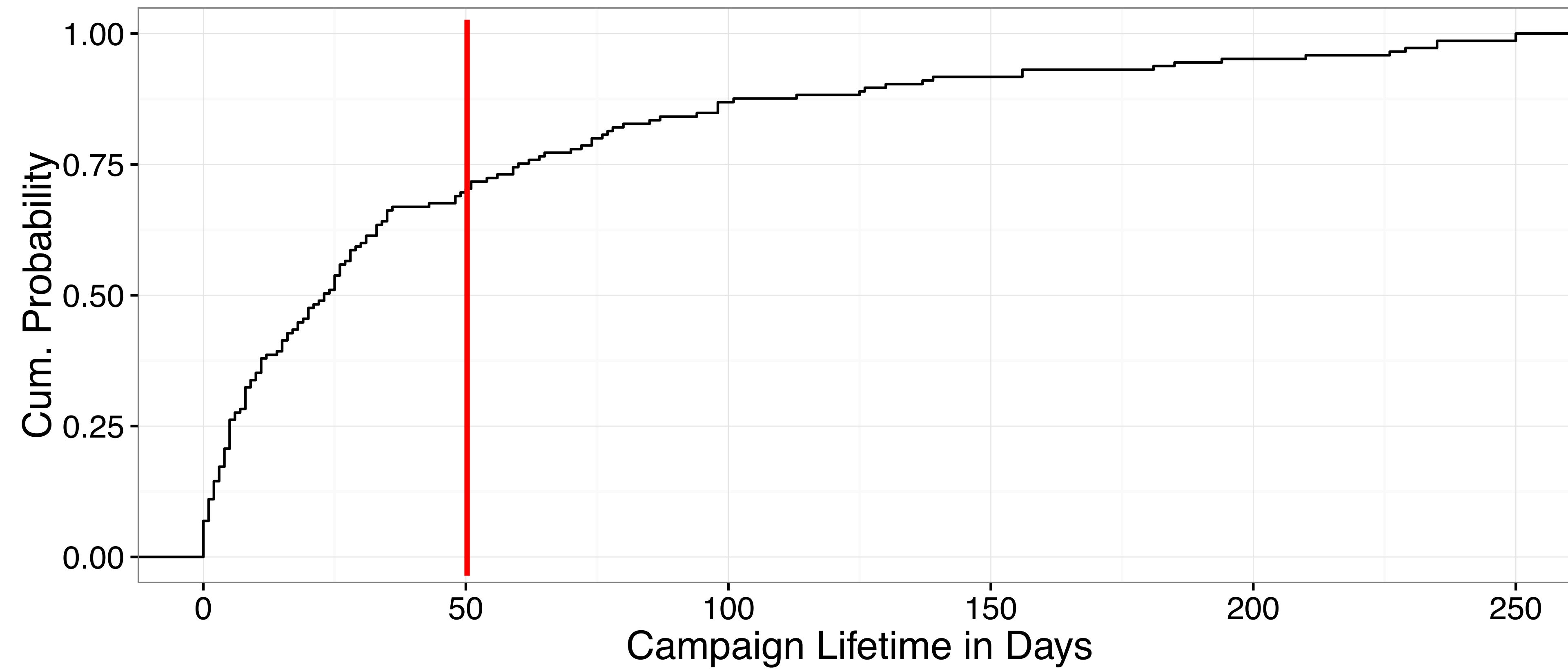
# Scam Campaigns

19



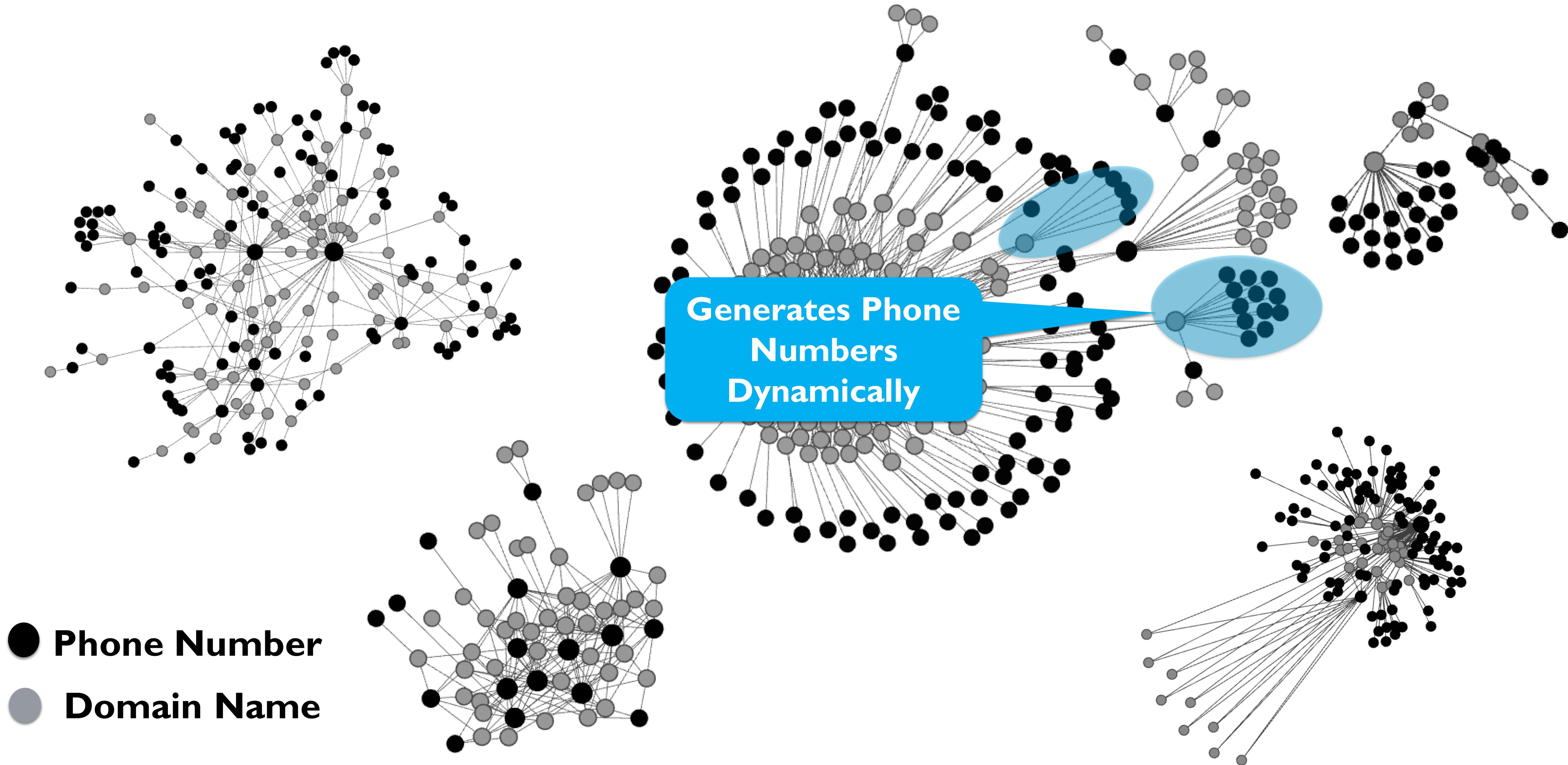
# Life time of Campaigns

20



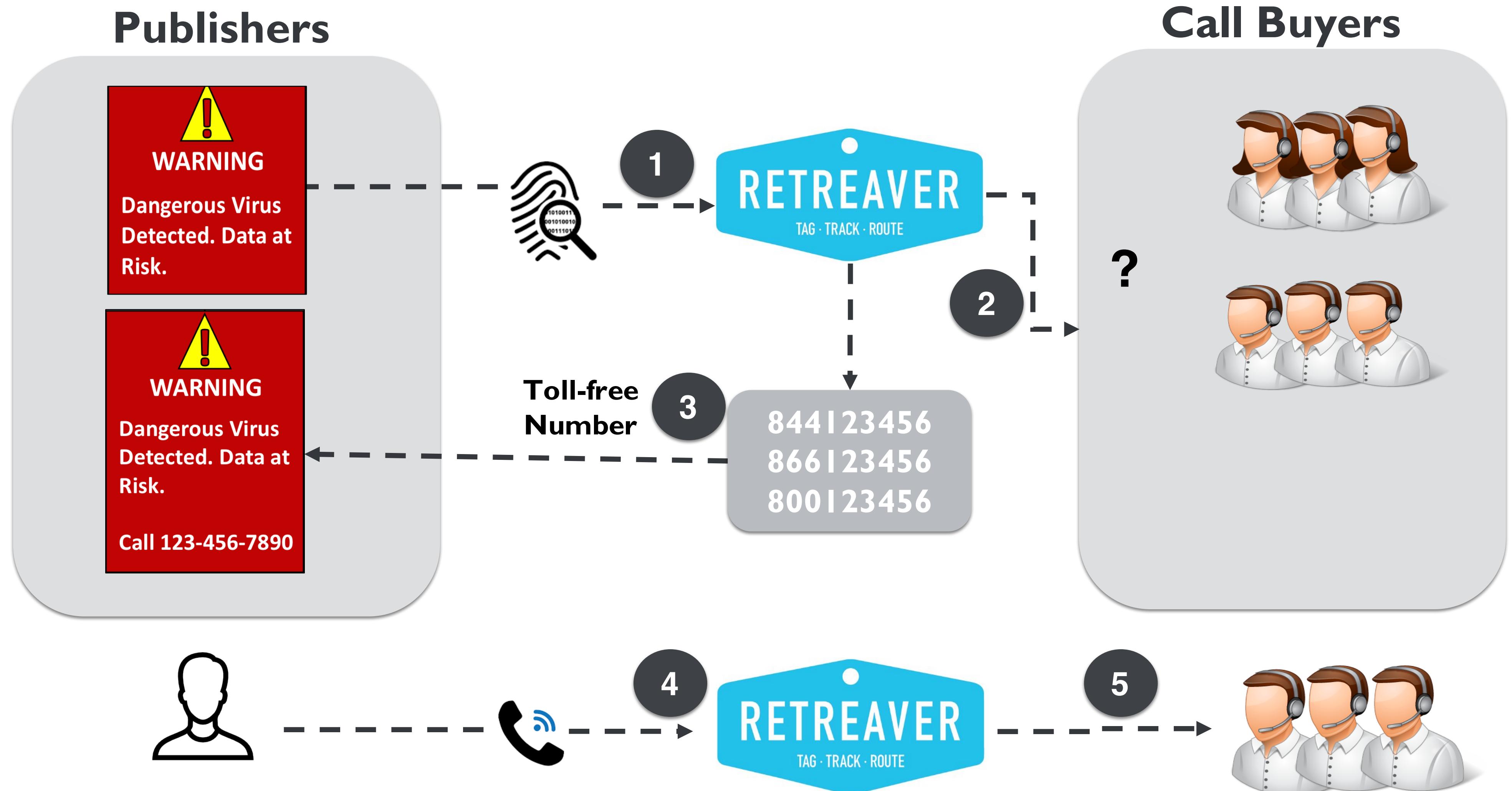
# Phone-TLD+1 Relationship

21



# Pay Per Call Marketing

22



# Meeting the Scammers

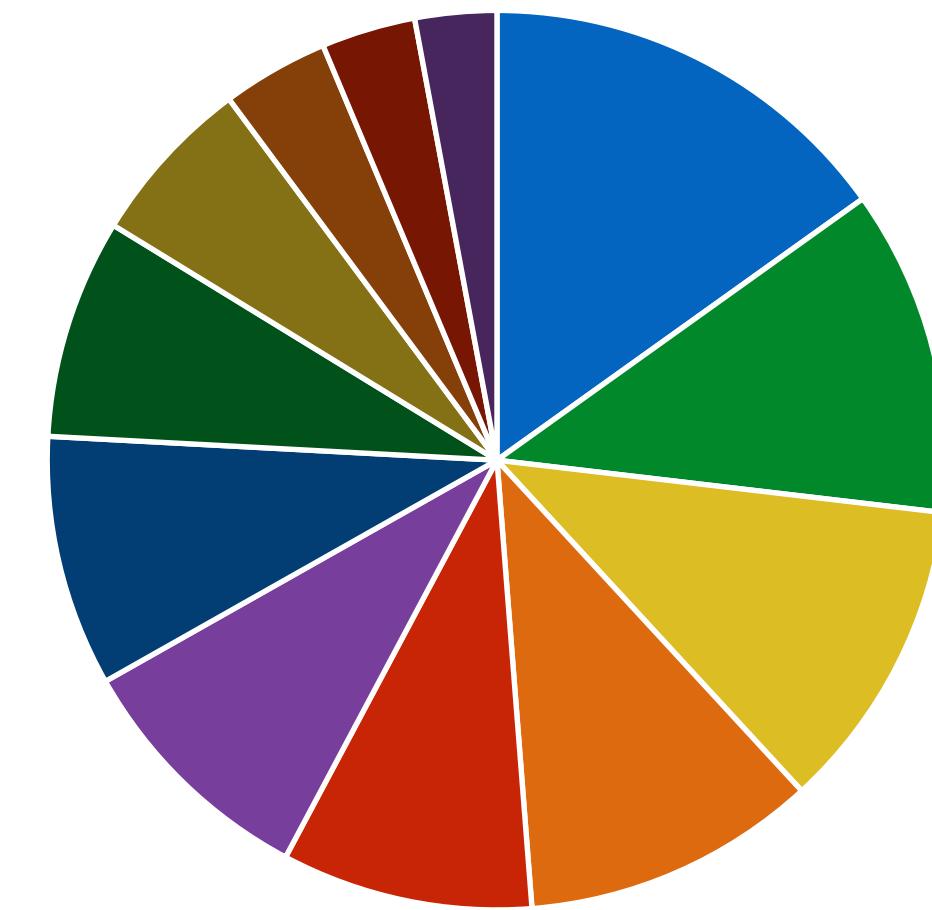
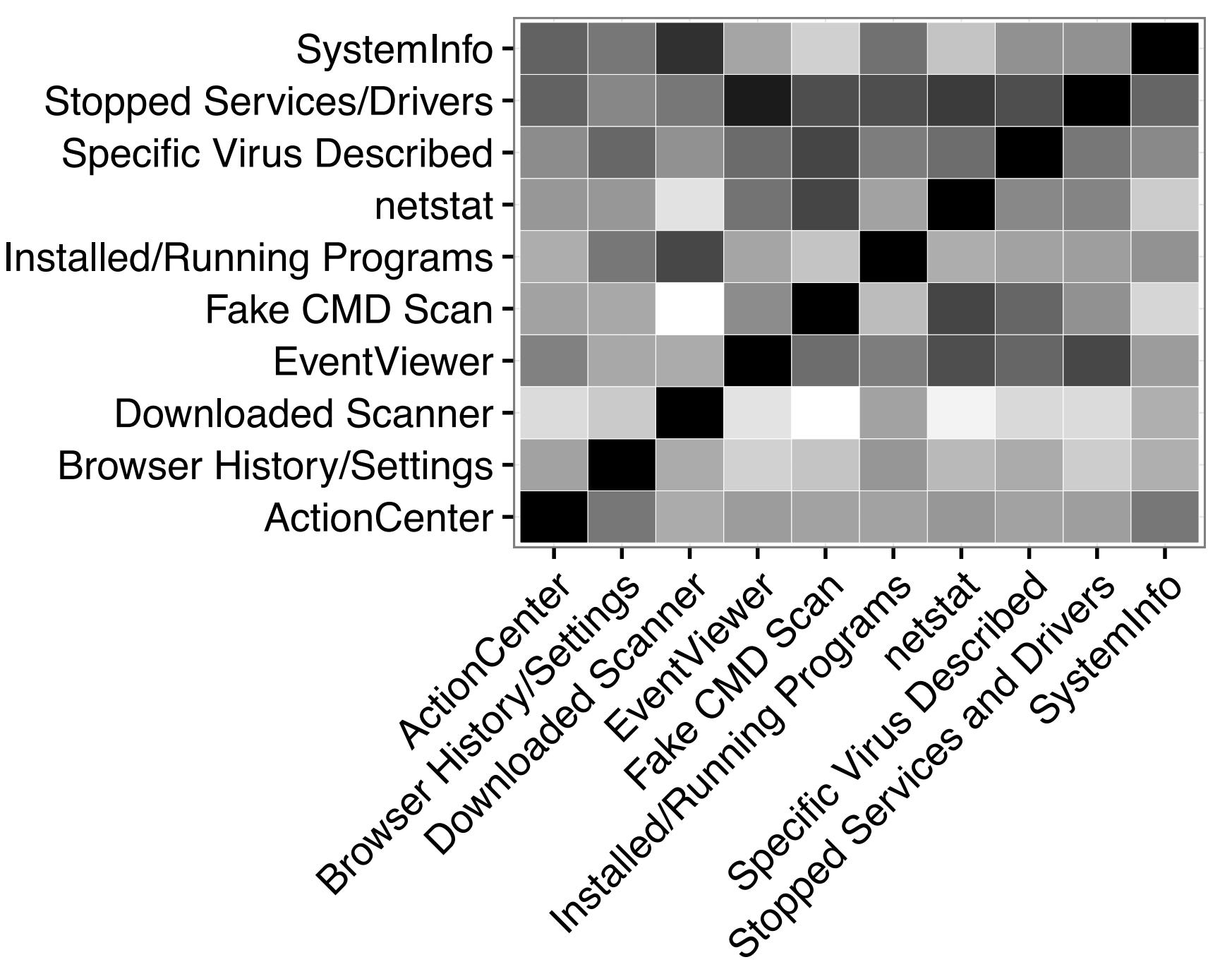
# Environment set up

24

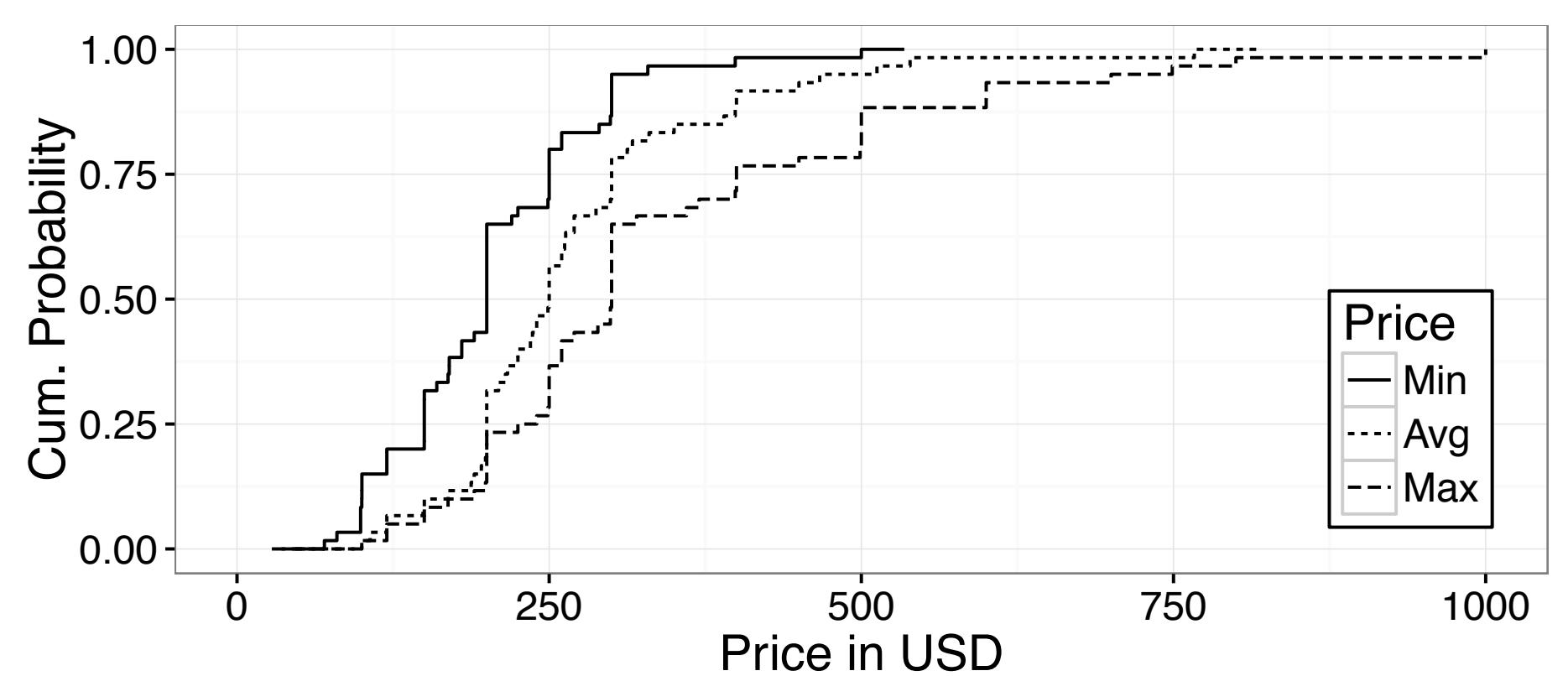
- Obtained permission from our IRB
- 60 interactions with the scammers
- Environment:
  - Artificially aged Windows 7 virtual machine
  - Tunneling the traffic through VPN
  - VoIP software with believable CallerID
  - Capturing network traffic, recording the screen and conversations

# Scammers' Tools & Techniques

25



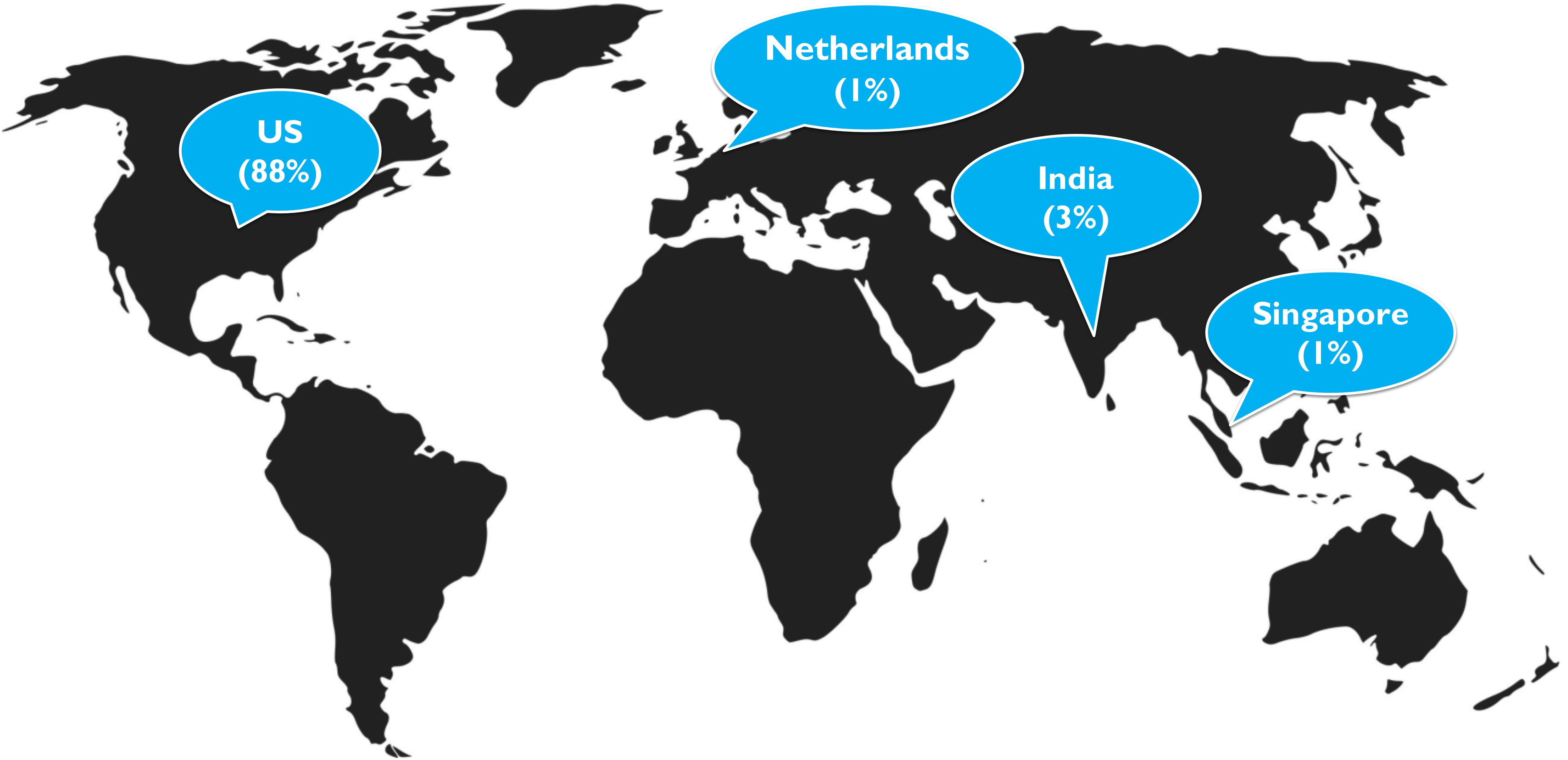
## Social Engineering Techniques



# Scammer Physical Locations & Profit

# Location of Scammers' Servers

27



# Location of Call Centers

28



# Number of Victims

29

- Monitoring Traffic of Scam Servers:
  - Misconfiguration of scam servers revealed their traffic
    - 142 scam domains were found which had misconfiguration
    - We monitored misconfigured servers every one minute over two months
  - Total visits : 1.7 million unique IPs
  - Max #visitors/domain : 138K unique IPs

# Location of Victims

30



# Scammers' Profit

31

Average price of Tech Support Scam Package (\$290)

\*

Number of Victims (1.7 million unique IPs)

\*

Conversion Rate (2% as a similar scareware)

---

Scammers' profit = ~ \$9.7 million in 2 months

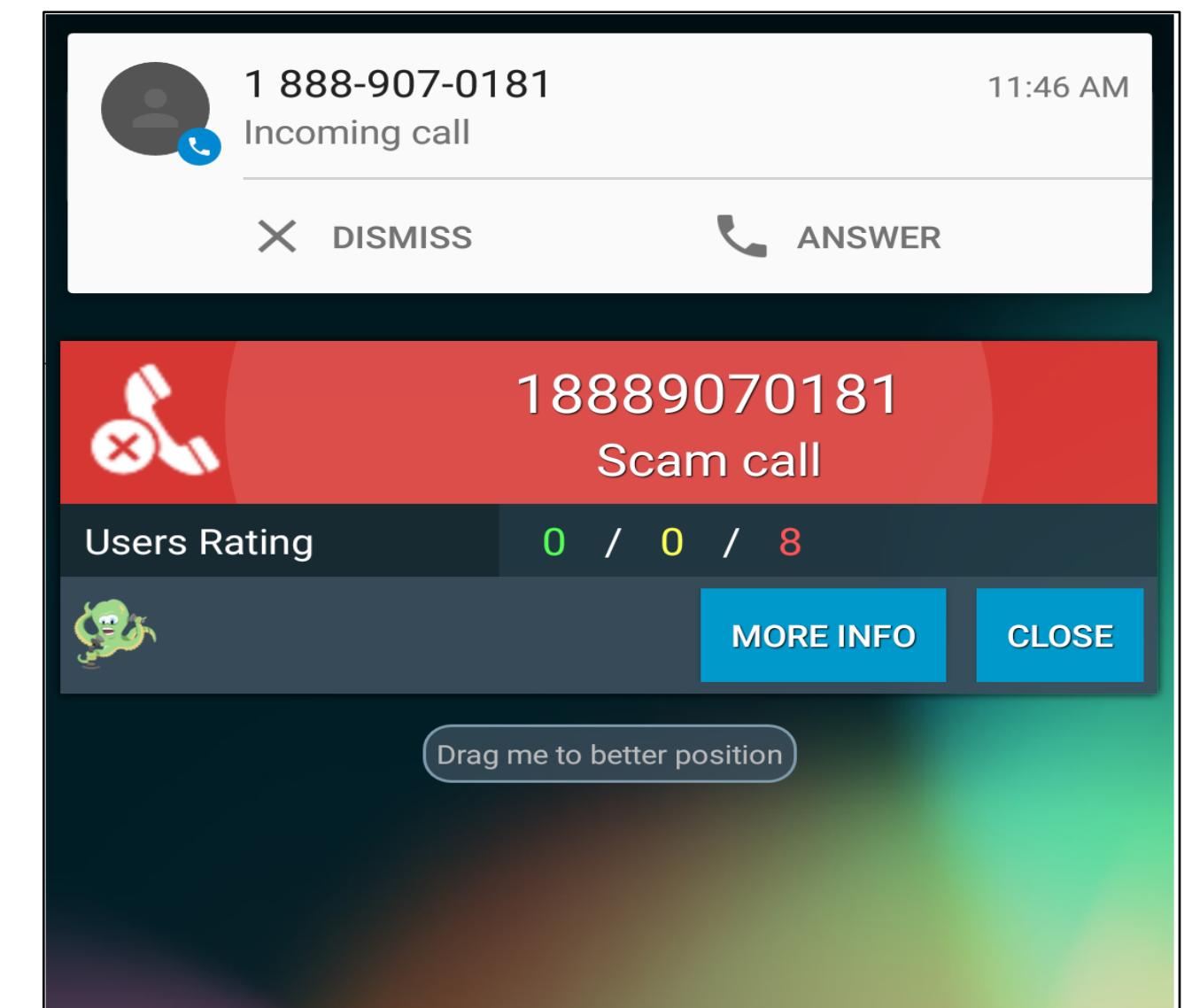
(a lower bound)

## Defense: Sufficiency of Current Blacklists

# Blacklists: Phone Numbers

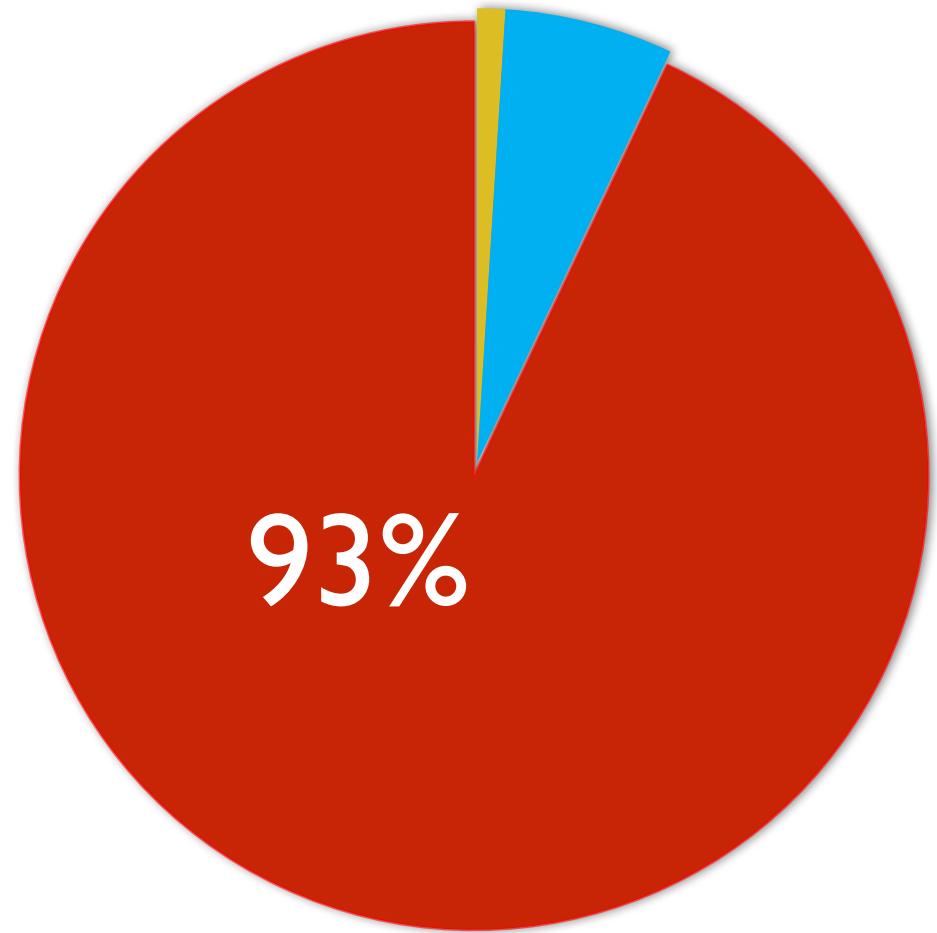
33

	Database	Coverage	Claimed Size
Website	mrnumber.com	19.9%	1.5 billion numbers
	800notes.com	18.5%	Unknown
	numberguru.com	1.0%	29 million lookups
	badnumbers.info	0.2%	968,639 complains
	callersmart.com	0.1%	5.9 million lookups
	scamnumbers.info	0.1%	31,162 numbers
Mobile App	Should I Answer?	0.5%	640 million lookups
	Truecaller	0.5%	2 billion numbers
	Hiya	0.3%	100 million numbers
	CallDetector	0.1%	100,000 complaints monthly
	Mr. Number	0.1%	1.5 billion numbers
	Together	27.4%	-



# Blacklists: Domain Names

34



- Detected Before Robovic
- Detected After Robovic
- Not Blacklisted

6 Blacklists (370K domains and IP addresses Together)

- hpHosts
- SANS suspicious domains
- malwaredomains
- malwaredomainlist
- Malc0de database
- abuse.ch

# Why do blacklists not work?

35

- Tech Support Scams are highly dynamic
  - 30% of the domains are alive less than a day
  - Abusing CDNs to get fresh URLs
  - Majority of phone numbers registered recently
  - Phone numbers are generated dynamically

# Defense against Tech Support Scam

36

- User Education
  - Explaining the concept of technical support scams is easier
  - Raising awareness through public services
- Browser Support
  - Average users do not know how to kill the browser process and clearing recent history
  - One universal shortcut to close unsafe pages



# Summary

37

- Tech support scams pose a serious threat
- We conducted the first systematic study of tech support scams
  - Reported prevalence of the scam and evasion techniques based on the collected corpus of thousands of domains and phone numbers
  - Clustered campaigns and estimated their life time
  - Interacted with 60 different scammers and identified the social engineering techniques
  - Underline the need for user education and support from the browser vendors

**nmiramirkhani@cs.stonybrook.edu**

# Dial One for Scam: A Large-Scale Analysis of Technical Support Scams

Najmeh Miramirkhani

Stony Brook University

nmiramirkhani@cs.stonybrook.edu

Oleksii Starov

Stony Brook University

ostarov@cs.stonybrook.edu

Nick Nikiforakis

Stony Brook University

nick@cs.stonybrook.edu

*Abstract*—In technical support scams, cybercriminals attempt to convince users that their machines are infected with malware and are in need of their technical support. In this process, the victims are asked to provide scammers with remote access to their machines, who will then “diagnose the problem”, before offering their support services which typically cost hundreds of dollars. Despite their conceptual simplicity, technical support scams are responsible for yearly losses of tens of millions of dollars from

Even though this type of scam costs users millions of dollars on a yearly basis [1], [2], there has been no systematic study of technical support scams from the security community. Thus, while today we know that these scams do in fact take place and that scammers are successfully defrauding users, any details about their operations are collected in an unsystematic way, e.g., by victimized users recalling their experiences, and